FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
09669/010001

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
09/936685

INTERNATIONAL APPLICATION NO. PCT/FR00/00680	INTERNATIONAL FILING DATE 17 March 2000	PRIORITY DATE CLAIMED 17 March 1999

TITLE OF INVENTION

METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES

APPLICANT(S) FOR DO/EO/US

Richard DOLLET

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)). (unsigned)
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

French Search Report (1 pg)

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/936685	PCT/FR00/00680	09669/010001

21. The following fees are submitted:.

CALCULATIONS PTO USE ONLY

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

- □ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**
- ☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO **$840.00**
- □ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**
- □ International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$670.00**
- □ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =				**$840.00**
Surcharge of **$130.00** for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492 (e)).	□ 20 □ 30			**$0.00**
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	8 - 20 =	0	x $18.00	**$0.00**
Independent claims	1 - 3 =	0	x $78.00	**$0.00**
Multiple Dependent Claims **(check if applicable)**.			□	**$0.00**
TOTAL OF ABOVE CALCULATIONS =				**$840.00**
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.	□			**$0.00**
SUBTOTAL =				**$840.00**
Processing fee of **$130.00** for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492 (f)).	□ 20 □ 30 +			**$0.00**
TOTAL NATIONAL FEE =				**$840.00**
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable)**.	□			**$0.00**
TOTAL FEES ENCLOSED =				**$840.00**

Amount to be: refunded	$
charged	$

☒ A check in the amount of **$840.00** to cover the above fees is enclosed.

□ Please charge my Deposit Account No. in the amount of to cover the above fees. A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **50-0591** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

ROSENTHAL & OSHA L.L.P.
700 Louisiana, Suite 4550
Houston, Texas 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8770

#45,925

SIGNATURE

Jonathan P. Osha
NAME

33,986
REGISTRATION NUMBER

9/17/01
DATE

ATTORNEY DOCKET NO. 09669/01001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Richard DOLLET	Art Unit:	
Serial No:		Examiner:	
Filed:	September 17, 2001		
Title:	METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES		

Assistant Commissioner for Patent
Washington, DC 20231

PRELIMINARY AMENDMENT

Dear Sir:

Prior to examination, please amend the application as follows:

IN THE SPECIFICATION

Page 1, between line 4 and line 5, insert: -- FIELD OF THE INVENTION--;

Page 1 between line 12 and line 13, insert: --BACKGROUND OF THE INVENTION--;

Page 2, between line 24 and line 25, insert: --SUMMARY OF THE INVENTION--;

Page 4, before line 1, insert: --BRIEF DESCRIPTION OF THE DRAWINGS--; and

Page 4, between line 13 and line 14, insert: --DETAILED DESCRIPTION--.

Please cancel Claim 3.

CLAIMS

1. (Amended) A method for secure loading of secret data from a first security module to at least one second security module, wherein said first module comprising at least one file of secret data, said second module comprises a first non-volatile memory and a second volatile memory, characterized in that it comprises the steps of:

- generating at least one random data item within the second memory in the second module,
- recording information comprising said random data item within the first memory of the second module,
- sending the random data item to the first module,
- within the first module, encrypting a secret data item in the file of said first module based on the random data item and an encryption algorithm,
- sending said encrypted secret data item to the second module,
- transferring information comprising the random data item stored in the first memory of the second module, from said first memory to the second memory of said module,
- decrypting said encrypted secret data item, based on a decryption algorithm and the random data item, and recording, within the second module, said decrypted secret data item.

2. (Amended) A method according to Claim 1, characterized in that it comprises a further step of:

   - after transferring the information comprising the random data item from the first memory of the second module in the second memory of said module, erasing said information from said first memory.

4. (Amended) A method according to Claim 1, characterized in that the steps of generating and sending the random data item as well as recording the information in the second module, are performed by means of a first command.

5. (Amended) A method according to Claim 1, characterized in that the steps of transferring information decrypting the secret data item in the second module and recording are performed by means of a second command.

6. (Amended) A method according to Claim 1, characterized in that the information which comprises said random data item, comprises an index relating to a secret data item.

7. (Amended) A method according to Claim 1, characterized in that several random data items are generated in the second memory of the second module and, after each random data item generation, information comprising the generated random data item is recorded in the first memory of the second module.

8. (Amended) A method according to Claim 1, characterized in that, on each loading operation, a random data item is used for loading a secret data item.

9. (Amended) A method according to Claim 1, characterized in that, on each loading operation, a unique random data item is used for loading several secret data items.

REMARKS

Full examination and favorable action are requested.

Please charge any fees, or make any credits, to Deposit Account No. 50-0591, Reference No. 09669/010001.

Date: 9/17/01

#45,925

Jonathan P. Osha
Reg. No. 33,986

Rosenthal & Osha L.L.P.
700 Louisiana Street, Suite 4550
Houston, TX 77002

Telephone: 713/228-8600
Facsimile: 713/228-8778

20033_1.DOC

APPENDIX A – MARKED-UP VERSION OF THE AMENDED CLAIMS

The material to be deleted is in brackets and in boldface.

CLAIMS

1. A method for secure loading of secret data from a first security module **[(S)]** to at least one second security module **[(SAM)]**, wherein said first module **[(S)]** comprising at least one file **[(EF1)]** of secret data **[(DATA)]**, said second module **[(SAM)]** comprises a first non-volatile memory **[(M1)]** and a second volatile memory **[(M2)]**, characterized in that it comprises the steps of:

   - generating at least one random data item **[(RAND)]** within the second memory **[(M2)]** in the second module **[(SAM)]**,
   - recording information **[(INFO)]** comprising said random data item **[(RAND)]** within the first memory **[(M1)]** of the second module **[(SAM)],**
   - sending the random data item **[(RAND)]** to the first module **[(S)]**,
   - within the first module **[(S)]**, encrypting a secret data item **[(DATA)]** in the file **[(EF1)]** of said first module **[(S)]** based on the random data item **[(RAND)]** and an encryption algorithm **[(ALGO)]**,
   - sending said encrypted secret data item **[(DATAC)]** to the second module **[(SAM)]**,
   - transferring information **[(INFO)]** comprising the random data item **[(RAND)]** stored in the first memory **[(M1)]** of the second module **[(SAM)]**, from said first memory **[(M1)]** to the second memory **[(M2)]** of said module **[(SAM)]**,
   - decrypting said encrypted secret data item **[(DATAC)]**, based on a decryption algorithm **[(ALGOP)]** and the random data item **[(RAND)]**, and recording, within the second module **[(SAM)]**, said decrypted secret data item **[(DATA)]**.

2. A method according to one of the preceding claims, characterized in that it comprises a further step of:
   - after transferring the information **[(INFO)]** comprising the random data item **[(RAND)]** from the first memory **[(M1)]** of the second module **[(SAM)]** in the second memory **[(M2)]** of said module, erasing said information **[(INFO)]** from said first memory **[(M1)]**.

4. A method according to any one of the preceding claims, characterized in that the steps of generating and sending the random data item **[(RAND)]** as well as recording the information **[(INFO)]** in the second module **[(SAM)]**, are performed by means of a first command **[(ASKLOADING)]**.

5. A method according to any one of the preceding claims, characterized in that the steps of transferring information **[(INFO)]** decrypting the secret data item **[(DATA)]** in the second module **[(SAM)]** and recording are performed by means of a second command **[(ADMINRECOVER)]**.

6. A method according to any one of the preceding claims, characterized in that the information **[(INFO)]** which comprises said random data item **[(RAND)]**, comprises an index relating to a secret data item **[(DATA)]**.

7. A method according to any one of the preceding claims, characterized in that several random data items **[(RAND)]** are generated in the second memory **[(M2)]** of the second module **[(SAM)]** and, after each random data item **[(RAND)]** generation, information **[(INFO)]** comprising the generated random data item **[(RAND)]** is recorded in the first memory **[(M1)]** of the second module **[(SAM)]**

8. A method according to any one of the preceding claims, characterized in that, on each loading operation, a random data item **[(RAND)]** is used for loading a secret data item **[(DATA)]**.

9. A method according to any one of claims 1 to 7, characterized in that, on each loading operation, a unique random data item **[(RAND)]** is used for loading several secret data items **[(DATA)]**.

METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES

The present invention relates to a method of secure loading of secret data from a first security module to at least one second security module, wherein said first module having at least one secret data file, said second module having a first non-volatile memory and a second volatile memory.

This invention can advantageously be applied to the field of telephony.

In the field of telephony, there are terminal administrating systems which comprise a first onboard security module within an administration server and second security modules generally onboard the above-mentioned terminals. The terminals are so-called public payphones.

A second security module guarantees the validity of a user card inserted into a public payphone, in particular by authenticating said card. For that purpose, the second security module comprises in its first memory secret data allowing said validity of user cards to be guaranteed. The public payphone administration systems as well as a secret data are managed by telephone companies. In order to reduce the risk of forgery consisting in tapping a communication network between the server and the public payphones and therefore to uncover said secret data, telephone companies are led to regularly modify all or part of the secret data in a second security module within a public payphone, based on secret data contained in a file in the first security module.

A known method of the art comprises steps of:

- encrypting the first security module's secret data which are to be transmitted to the second security module and reside in the managing server,

- causing the public payphone to connect to the administrating server when there is no ongoing call,
- transmitting the secret data to the second security module within the public payphone.

When the public payphone connects to the administrating server, it is unavailable to any user, so that this connection generally occurs during the night. The data exchange is done in the so-called "off-line" disconnected mode.

In order to diversify the transmissions of secret data, a pseudo-random piece of data is used based on the value of a counter in the second security module. On each secret data exchange, the counter value is incremented, and the first security module has to know the value of said counter and increment a local counter dedicated to the second module.

Although this method allows secret data to be loaded between first and second security modules, it requires heavy data base administration for ensuring proper synchronization of the different counters. Specifically, track must be kept of all exchanges carried out with a second security module. Moreover, this method does not ensure a perfectly diversified data exchange.

Thus, a technical problem to be solved by the present invention is to provide a method of secure loading of secret data from a first security module to at least one second security module, wherein said first module comprises at least one secret data file, said second module comprises a first non-volatile memory and a second volatile memory that would ensure a perfectly diversified data exchange between first and second security modules in the off-line mode while avoiding excessive data base management.

According to the present invention, a solution to the technical problem posed is such as the loading method comprises the steps of:

- generating at least one random data item within the second memory in the second module,
- recording information comprising said random data item within a first memory of the second module,
- sending the random data item to the first module,
- within the first module, encrypting a secret data item of the file in said first module based on the random data item and an encryption algorithm,
- sending said encrypted secret data item to the second module,
- transferring information comprising the random data item stored in the first memory of the second module, from said first memory to the second memory of said module,
- decrypting said encrypted secret data item based on a decryption algorithm and the random data item and recording, within the second module said decrypted secret data item.

Thus, as shown in detail below, the loading method according to the present invention allows, by using a random data item for loading secret data, to improve data loading security by perfectly diversifying the transmitted data. Thus, a defrauder spying on the communication network and collecting the transmitted data will never be able to obtain the same encrypting value and therefore will never be able to uncover any secret relating to the transmitted secret data. In addition, recording the random data item within a non-volatile memory in the second security module, allows it to be used in the "off-line" mode, since said random data item is not lost when said second security module is turned off.

Other features and advantages of the invention will become apparent in the following description of preferred embodiments of the present invention, which are provided by way of non limiting examples in reference to the appended figures.

Figure 1 is a view of a first security module and several second security modules.

Figure 2 is a diagram showing the first module and the second module of Figure 1.

Figure 3 is a diagram showing a data exchange between the first module and the second module of Figure 2.

Figure 4 is a diagram showing a first data exchange between the first module and the second module of Figure 2.

Figure 5 is a diagram showing a third data exchange between the first module and the second module of Figure 2.

In Figure 1, there is shown a first security module S and several second security modules SAM, each second module SAM comprising a first non-volatile memory M1 and a second volatile memory M2 referred to as the work memory. Figure 2 shows the first module S and a second module SAM. The first module S includes at least one file EF1 storing secret data DATA and an encrypting algorithm ALGO. A secret data file is generally associated with a given telephone company. The second module SAM comprises a decryption algorithm ALGOP which is the reverse of the encryption algorithm ALGO, and secret data DATA.

In order to change a secret data item within the second module SAM, a secret data item has to be loaded from the file EF1 within the first security module S. The loading operation should be performed in a secure way. The secret data item is thus transmitted after encryption. The loading phase comprises several steps, as described below.

In a first step, at least one random data item RAND is generated within volatile memory M2 of the second module SAM.

In a second step, as shown in Figure 3, information INFO comprising said random data item RAND is recorded into non-volatile memory M1 of the second module SAM. A memory location within said non-volatile memory M1 is set aside for that purpose and is set to its default initialization value V.

In a first embodiment, information INFO, which comprises said random data item RAND, includes an index pertaining to a secret data item DATA. This index can for example be the number of a secret piece of data to be modified or and index of a memory location where a secret data item should be loaded into a second module SAM. Thus, when the second module SAM is turned-off for power saving reasons, the random data item RAND and its associated information are not lost.

In a third step, the random data item RAND is sent to the first module. It should be noted that the second and third steps are interchangeable.

In order to reduce the number of accesses to the second module SAM, generating and sending the random data item RAND as well as recording information INFO into the second module SAM, are carried out by means of a first command ASKLOADING. This first command is sent by the administrating server to the second module SAM via the public payphone (not shown).

In a fourth step, in the first module S, the secret data item DATA in file EF1 to be transmitted to the second module SAM is encrypted. This encryption comprises an encryption step using the encryption algorithm ALGO and the random data item RAND. Using the random data item RAND avoids having the same encryption value for a secret data item DATA. Thus, is will be difficult for a defrauder to find any relation between the different data items transmitted over the communication network since they are different from one transmission to the next. The encryption can also comprise, on the one hand, a step of signing the secret data item DATA based on the random data item RAND and, on the other hand, a step of certifying the transmitted data. The signature step allows the authenticity of the loaded secret data item DATA to be checked and the certificate allows transmitted data integrity to be checked.

In a fifth step, as shown in Figure 4, said encrypted secret data item DATAC is sent to the second module SAM.

In a sixth step, information INFO, comprising the random data item RAND stored in non-volatile memory M1 of the second module SAM, is transferred from said memory M1 to the work memory M2 of said module SAM. Thus, the random data item RAND which was used for encrypting the secret data item DATA, as well as its associated information, are recovered from work memory M2.

Duplicating the random data item RAND and its associated information into two different memories of the second module SAM may lead to discrepancies within said module and security issues. Therefore, only one set of information INFO is kept in the second module SAM. For that purpose, after recording information INFO, which comprises said random data item RAND within the first memory M1 of the second module SAM (Figure 3), the information INFO stored in the second memory M2 of said second module SAM is deleted. Similarly, after transferring information INFO comprising the random data item RAND from the first memory M1 of the second module SAM into the second memory M2 of said module (Figure 4), information INFO stored within the first memory M1 is deleted.

Finally, in a last step, said encrypted secret data item DATAC is decrypted based on the decryption algorithm ALGOP of the second module SAM and on the random data item RAND, and said decrypted secret data item DATA is recorded into the second module SAM.

In order to reduce the number of accesses to the second module SAM, the steps of transferring information INFO, decrypting secret data item DATA within the second module SAM and recording are performed by means of a second command ADMINRECOVER. This second command is sent by the administrating server to the second module SAM via the public payphone (not shown). In case a fault occurs during the loading operation or at the end of said loading operation, the memory location within non-volatile memory M1 where information INFO comprising the random data item RAND is stored, is reset to its initialization value V. If a fault has occurred, another random data item RAND is generated and the different steps of the above-described method are performed again. When the second ADMINRECOVER command is sent, it is checked whether a random data item RAND has been generated and recorded. Thus, it is checked whether the memory location of the first non-volatile memory M1 in the second module SAM, dedicated to the random data item RAND, contains the initialization value V. If it does, the second ADMINRECOVER command is executed. In the opposite case, it is not executed and the first step of the method is performed.

Generally, a second SAM module will manage different types of user cards and therefore comprise several secret data items associated with each type of user card, a card type generally corresponding to a given company, that provides said cards. Usually, it is desirable to be able to modify the set of secret data item DATA associated with a given card type. In this case, the first steps of the method according to the invention as described above are performed, but are applied to all of the secret data item DATA to be modified. Thus, several random data item RAND are generated within the second memory M2 of the second module SAM and the information INFO comprising the generated random data item RAND is recorded after each generation of a random data item RAND. As shown in the example of Figure 5, three random data items RAND1, RAND2 and RAND3 are generated within the second module SAM and are recorded into non-volatile memory M1 of said module. Accordingly, the three generated random pieces of data are sent to the first module S1 in the administrating server. Three secret data items DATA1, DATA2 and DATA3 residing in file EF1 in the first module F are encrypted and correspond to the three secret data items to be modified within the second module SAM. They are matched, for example, by means of three indices (1, 2 and 3) of secret data sent at the same time as the three random data items RAND. Finally, for transmitting the three secret data items DATA1, DATA2 and DATA3, in said second module SAM, the steps of the method according to the invention as described above are all performed from the fifth step for each secret data item to be loaded or for the whole set of secret data as in the previous steps.

Therefore, according to a first embodiment for loading several data items as described above, on each loading operation, a random data item RAND is used for loading a secret data item DATA. According to a second embodiment, in order to reduce the time required for loading the secret data, on each loading operation, a unique random data item RAND is used for loading several secret data items DATA.

Of course, the present invention is not restricted to the field of telephony, and can be applied to other fields wherein a data exchange system is implemented between a centralized module storing secret data and remote modules adapted to receive such secret data.

CLAIMS

1. A method for secure loading of secret data from a first security module (S) to at least one second security module (SAM), wherein said first module (S) comprising at least one file (EF1) of secret data (DATA), said second module (SAM) comprises a first non-volatile memory (M1) and a second volatile memory (M2), characterized in that it comprises the steps of:

- generating at least one random data item (RAND) within the second memory (M2) in the second module (SAM),
- recording information (INFO) comprising said random data item (RAND) within the first memory (M1) of the second module (SAM),
- sending the random data item (RAND) to the first module (S),
- within the first module (S), encrypting a secret data item (DATA) in the file (EF1) of said first module (S) based on the random data item (RAND) and an encryption algorithm (ALGO),
- sending said encrypted secret data item (DATAC) to the second module (SAM),
- transferring information (INFO) comprising the random data item (RAND) stored in the first memory (M1) of the second module (SAM), from said first memory (M1) to the second memory (M2) of said module (SAM),
- decrypting said encrypted secret data item (DATAC), based on a decryption algorithm (ALGOP) and the random data item (RAND), and recording, within the second module (SAM), said decrypted secret data item (DATA).

2. A method according to one of the preceding claims, characterized in that it comprises a further step of:

- after transferring the information (INFO) comprising the random data item (RAND) from the first memory (M1) of the second module (SAM) in the second memory (M2) of said module, erasing said information (INFO) from said first memory (M1).

3. A method according to any one of the preceding claims, characterized in that it comprises a further step of:

- after transferring the information (INFO) comprising the random data item (RAND) from the first memory (M1) of the second module (SAM) in the second memory (M2) of said module erasing said information (INFO) from said first memory (M1).

4. A method according to any one of the preceding claims, characterized in that the steps of generating and sending the random data item (RAND) as well as recording the information (INFO) in the second module (SAM), are performed by means of a first command (ASKLOADING).

5. A method according to any one of the preceding claims, characterized in that the steps of transferring information (INFO) decrypting the secret data item (DATA) in the second module (SAM) and recording are performed by means of a second command (ADMINRECOVER).

6. A method according to any one of the preceding claims, characterized in that the information (INFO) which comprises said random data item (RAND), comprises an index relating to a secret data item (DATA).

7. A method according to any one of the preceding claims, characterized in that several random data items (RAND) are generated in the second memory (M2) of the second module (SAM) and, after each random data item (RAND) generation, information (INFO) comprising the generated random data item (RAND) is recorded in the first memory (M1) of the second module (SAM).

8. A method according to any one of the preceding claims, characterized in that, on each loading operation, a random data item RAND is used for loading a secret data item DATA.

9. A method according to any one of claims 1 to 7, characterized in that, on each loading operation, a unique random data item RAND is used for loading several secret data items DATA.

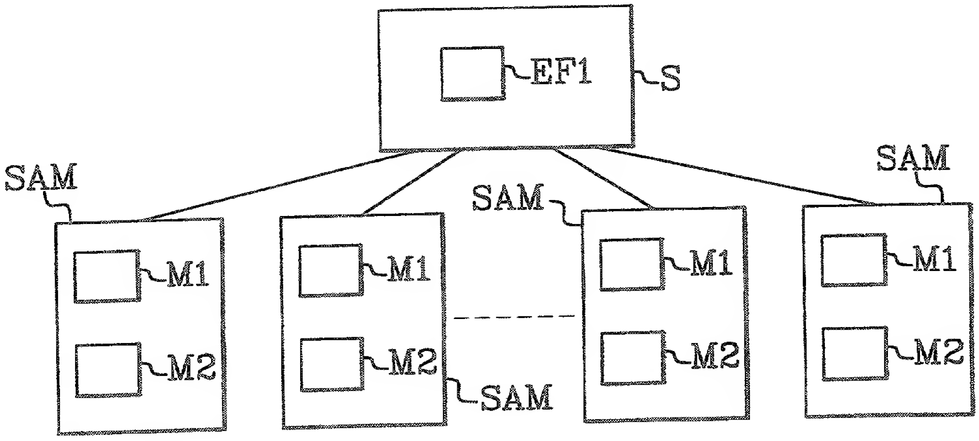

FIG.1

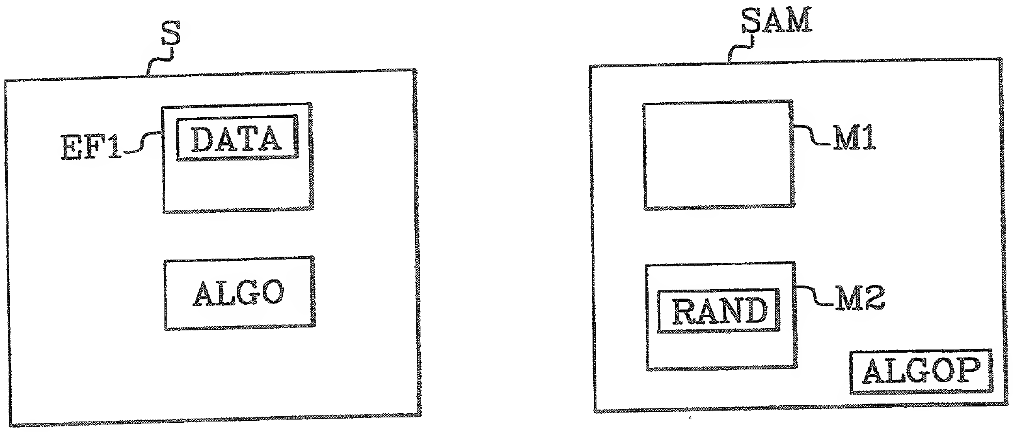

FIG.2

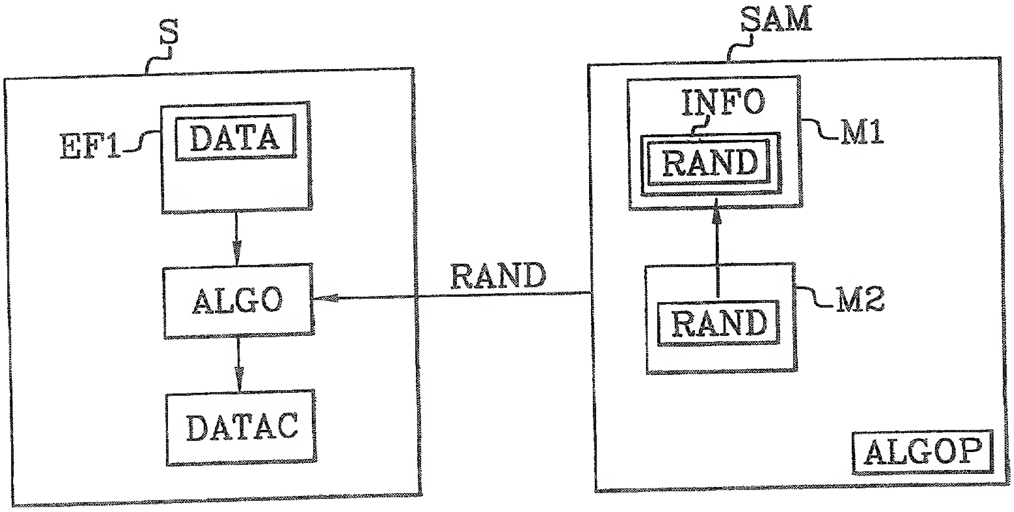

FIG.3

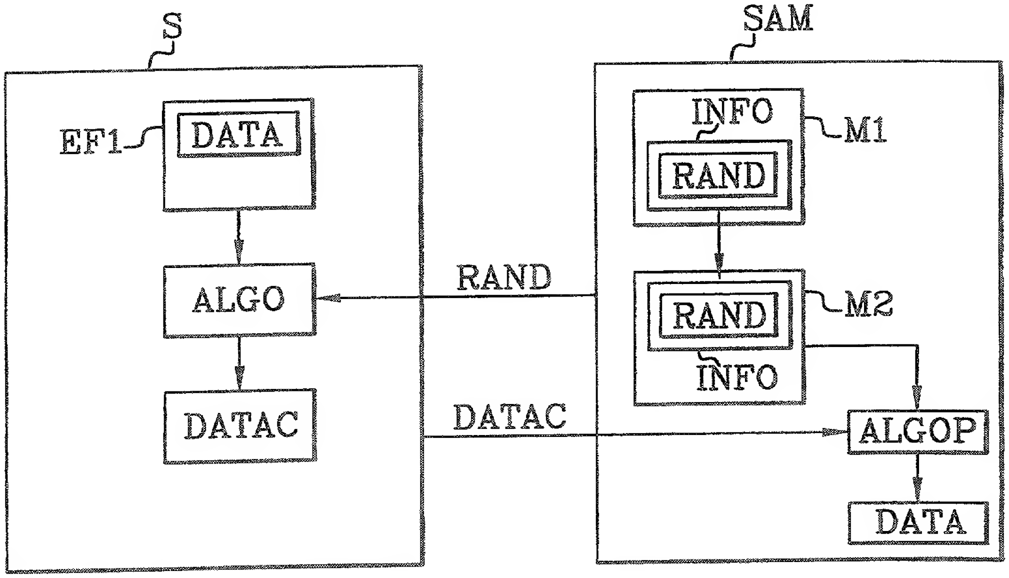
S
SAM
EF1
DATA
ALGO
DATAC
RAND
DATAC
INFO
RAND
M1
RAND
INFO
M2
ALGOP
DATA

FIG.4

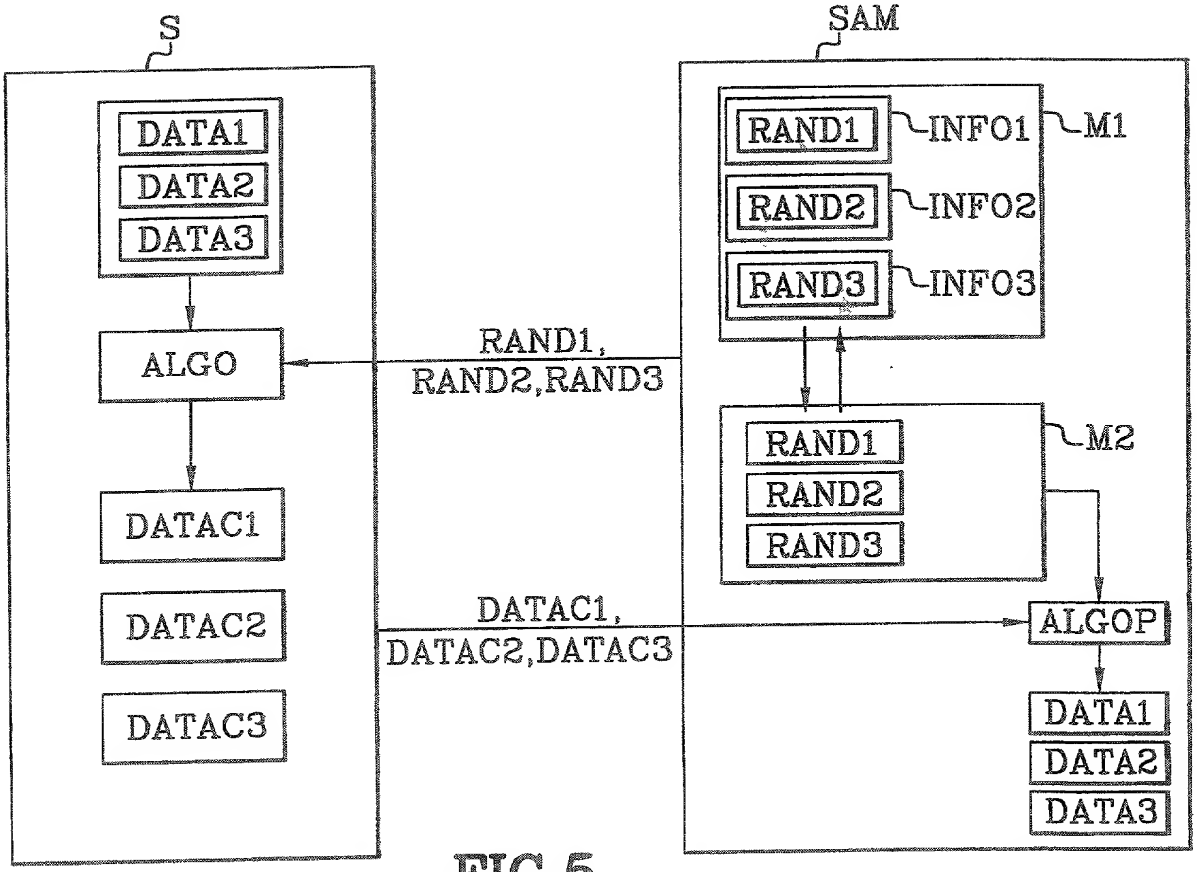
S
SAM
DATA1
DATA2
DATA3
ALGO
DATAC1
DATAC2
DATAC3
RAND1,
RAND2,RAND3
DATAC1,
DATAC2,DATAC3
RAND1
INFO1
M1
RAND2
INFO2
RAND3
INFO3
RAND1
RAND2
RAND3
M2
ALGOP
DATA1
DATA2
DATA3

FIG.5

PTO/SB/01 (03-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

□ Declaration Submitted with Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	09669/010001
First Named Inventor	DOLLET
COMPLETE IF KNOWN	
Application Number	09/936, 685
Filing Date	September 17, 2001
Group Art Unit	
Examiner Name	

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES.

(Title of the Invention)

the specification of which

□ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 09/ 17/ 2001 as United States Application Number or PCT International

Application Number 09/ 936, 685 and was amended on (MM/DD/YYYY) ______ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
99/ 03329	France	03/ 17/ 1999	□	□	☒
			□	□	□
			□	□	□
			□	□	□

□ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒ Customer Number or Bar Code Label 22511 PATENT TRADEMARK OFFICE		OR ☐ Correspondence address below	
Name			
Address			
City		State	ZIP
Country	Telephone		Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR : ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]) Richard		Family Name or Surname DOLLET	
Inventor's Signature			Date 10/12/2001
Residence: City Paris	State FRX	Country France	Citizenship French
Mailing Address 50, Avenue Jean Jaurès – B.P. 620-12			
City Montrouge Cedex	State	ZIP 92542	Country France

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])		Family Name or Surname	
Inventor's Signature			Date
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	ZIP	Country

☐ Additional inventors are being named on the ____supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.